

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 63-146631

(43)Date of publication of application : 18.06.1988

(51)Int.Cl.

H04L 9/04

G09C 1/00

(21)Application number : 61-295342

(71)Applicant : NEC CORP

(22)Date of filing : 10.12.1986

(72)Inventor : OKAMOTO EIJI

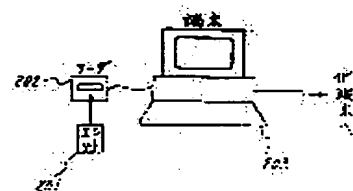
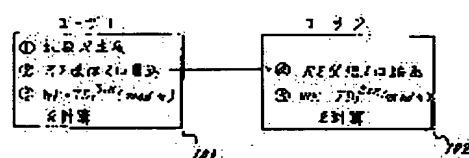
(54) KEY GENERATING DEVICE

(57)Abstract:

PURPOSE: To generate a cryptographic key with high in secrecy by converting a random number selected at random, a select code preserved by it own equipment only, identification information of opposite station and a common code to all stations by predetermined conversion.

CONSTITUTION: Identification information IDi of a user (1) is the result of coding public information such as name, address and telephone number to identify the user (1). Moreover, a secret integer Si processed by the user (1) only and product (n) of plural primes are calculated by a credible manager and arranged in advance to the user (1). The user (1) inputs a cryptographic communication request to a terminal equipment 203 and loads an IC card 201 to a reader 202. The terminal equipment generates a random number R, reads the S1 and (n) from the IC card 201 to generate a work key wk, which ciphers a message desired to be sent and the result is sent to the user 2 together with the number R.

In receiving the R and the ciphered message, the user 2 reads the S1 and (n) from the IC card to generate the work key wk. Then the wk is used to decode the sent ciphered message into the original plain sentence.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A) 昭63-146631

⑬ Int.Cl.⁴

識別記号

庁内整理番号

⑭ 公開 昭和63年(1988)6月18日

H 04 L 9/04
G 09 C 1/00

7240-5K
7368-5B

審査請求 未請求 発明の数 2 (全4頁)

⑮ 発明の名称 キー生成装置

⑯ 特 願 昭61-295342

⑰ 出 願 昭61(1986)12月10日

⑱ 発 明 者 岡 本 栄 司 東京都港区芝5丁目33番1号 日本電気株式会社内
⑲ 出 願 人 日本電気株式会社 東京都港区芝5丁目33番1号
⑳ 代 理 人 弁理士 内 原 晋

明 細 書

発明の名称

キー生成装置

特許請求の範囲

1. 複数の局から成る通信ネットワークの1つの局と他の局との間の暗号用のキーを生成するキー生成装置において、ランダムに選ばれた乱数と、自局のみが保有する秘密コードと、相手局の識別情報と、全局に共通なコードとをあらかじめ定められた変換で変換して前記暗号用のキーを生成することを特徴とするキー生成装置。

2. 記録情報を暗号化あるいは復号化するときのキーを生成するキー生成装置において、ランダムに選ばれた乱数と、ユーザ固有の秘密コードと、全ユーザに共通なコードと、ユーザ識別情報とをあらかじめ定められた変換で変換して前記キーを生成することを特徴とするキー生成装置。

発明の詳細な説明

(産業上の利用分野)

本発明は通信暗号あるいはファイル暗号に用いるキーを生成するキー生成装置に関する。

(従来の技術)

キー生成装置として従来から知られているものの1つに、公開鍵配送方式を用いたキー生成装置がある。この方式はアイ・イー・イー・イー・トランザクションズ・オン・インフォメーション・セオリー (IEEE Transactions on Information Theory) 22巻 6号 644頁～654頁に掲載されている。

このキー生成装置は各通信者(またはファイルの寄込者や読出者、以下通信者に含める)に対応した公開情報が必要とし、例えば通信者Aが通信者Bと暗号通信する場合には、AはBの公開情報 Y_B とAのみの秘密情報 X_A から $Y_B^{X_A} \pmod{p}$ により暗号キー wk を作成する。ここで、 p は公開されている大きな素数(256ビット程

特開昭63-146631(2)

度)であり、 $a \pmod{b}$ は a を b で割った余りを示す。Bは同様に $Y_A^{X_B} \pmod{p}$ により wk を作成する。

ここで $Y_A^{X_A} \pmod{p} = Y_A^{X_B} \pmod{p}$ となるように $Y_A = \alpha^{X_A} \pmod{p}$ 、 $Y_B = \alpha^{X_B} \pmod{p}$ と定められている。 α は定数。

Y_A と α と p がわかっていても、 $Y_A = \alpha^{X_A} \pmod{p}$ をみたす X_A を求めることは困難であること、即ち、いわゆるディスクリート・ログリズムの困難さが前記文献に記載されている。

(発明が解決しようとする問題点)

前記の従来のキー生成装置では、各通信者に対応する公開情報が必要となり、メンバーが増加すれば公開情報のリストも増加する。また、改ざんなども防止するための管理が必要となる。これらの欠点はファイル暗号の時も同様に存在する。

本発明の目的は、簡単な手段により上記欠点を除去し、機密性の高い暗号用のキーを生成することのできるキー生成装置を提供することにある。
(問題点を解決するための手段)

第1の発明のキー生成装置の構成は、複数の局から成る通信ネットワークの1つの局と他の局との間の暗号用のキーを生成するキー生成装置において、ランダムに選ばれた乱数と、自局のみが保有する秘密コードと、相手局の識別情報と、全局に共通なコードとをあらかじめ定められた変換で変換して前記暗号用のキーを生成することを特徴とする。

第2の発明のキー生成装置の構成は、記録情報を暗号化あるいは復号化するときのキーを生成するキー生成装置において、ランダムに選ばれた乱数と、ユーザ固有の秘密コードと、全ユーザに共通なコードと、ユーザ識別情報とをあらかじめ定められた変換で変換してキーを生成することを特徴とする。

(実施例)

第1図は第1および第2の発明の一実施例の原理を示すための図である。

第1の発明における局は端末、ユーザ等の通信主体であるが、第2の発明の主体であるユーザという言葉を共通に用いる。

第1図は第1の発明と第2の発明の共通原理を示している。キー配送の起動をかける側あるいはファイル書込を行なう側をユーザ1とし他方をユーザ2とする。ユーザ1は乱数 R を生成し、 R をユーザ2に送るか、ファイルの1部に書込む。

次に、暗号用のキー(以下ワークキーと言う)を、 $wk = ID_2^{S_1 R} \pmod{n}$ で計算する。

ここで、 n は複数の素数の積 $p_1 p_2 \dots p_k$ であり、約200桁程度の大きな整数である。

また、 ID_1 はユーザ1の識別情報で、例えば、氏名、住所、電話番号など、ユーザ1を識別できる公開の情報をコード化して整数とみなしたものである。

さらに、 S_1 はユーザ1のみが保有する秘密の

整数である。これらの S_i 、 n は信頼できる管理者が計算してユーザ1にあらかじめ配っておく。この計算の仕方は後に示す。ユーザ2も同様にして、ワークキー wk を、 $wk = ID_1^{S_2 R} \pmod{n}$ により計算する。ここで、 ID_1 と S_1 の関係は

$$ID_1 = \alpha^{S_1} \pmod{n} \quad (1)$$

となっている。 α はある整数。このときユーザ1とユーザ2が計算したワークキー wk は、共に $\alpha^{S_1 S_2 R} \pmod{n}$ に等しくなる。

ここで、 ID_1 、 α 、 n がわかっていても、 n が大きいために S_1 を求めることができない。従って、ユーザ1とユーザ2以外の第三者が R を知っても、 $\alpha^{S_1 S_2 R} \pmod{n}$ を作れない。これらは、ディスクリート・ログリズムの困難さによる。

一方、管理者は n の因数 p_1, p_2, \dots, p_k を各々小さくしておけば、任意の ID に対して

特開昭63-146631(3)

$$ID = \alpha^{x_j} \pmod{p_j} \quad (2)$$

をみたす x_j を計算できる。

ここで、 α は $\pmod{p_j}$ において生成元となるような任意の整数とする。

具体的な x_j の計算法については、例えば第20回アニュアル・シンポジウム・オン・ファウンデーションズ・オブ・コンピュータ・サイエンス (Annual Symposium on Foundations of Computer Science) 予稿集の56頁～60頁 (1979) に記載されている。

第2図は本発明の第1の実施例の構成を示すための図である。

ネットワークの端末203にICカード・リーダー202が設置されている。ICカード201は管理者が秘密のコード S_i および公開の整数 n を書き込んで各ユーザに配布したものである。

端末203がなすべき作業を第3図にフローチャートにして示す。ユーザ1がユーザ2に暗号通信を行なうものとして説明する。

ユーザ1は端末203に暗号通信要求を入力すると共に、ICカード201をリーダー202に差し込む。すると端末はユーザ1の正当性をチェックする。これは、ICカードの正当性チェックを利用すればよく、例えば、暗証番号をICカードの読み書きできないメモリエリアにICカード製作段階に記入しておき、ユーザ1が端末に入力した暗証番号と一致するか否かでユーザ1の正当性を判定する。一致すれば、端末は乱数 R を生成し、ICカード201から S_i と n を読み込む。

ワークキー w_k を式(1)に基づいて生成し、ワークキー w_k で送りたいメッセージを暗号化して、その暗号文を前記 R と共にユーザ2へ送る。ユーザ2は R と暗号文を受取ると、端末が同様にユーザ2の正当性をチェックし、チェックが肯定的になされた時は、ICカードから S_i と n を読み込んでワークキー w_k を生成する。そして、その w_k を用いて送られた暗号文を元の平文に戻す。

第4図は第2の実施例の構成を示すための図である。第2図における端末203をフロッピーデ

ィスク付パーソナルコンピュータ (パソコン) としている。動作は第2図における通信文がフロッピーディスクへの記録文になったことだけである。但し、暗号化するユーザと復号化するユーザが同一であり得る点が、第2図と異なる。

本実施例において、フロッピーディスクやパソコンは一例にすぎず、他の記録媒体やコンピュータでもよい。

〔発明の効果〕

以上詳細に説明したように、本発明を用いれば、各ユーザに対応して公開情報をリストにしたテーブルが不要となる効果をもたらす。

図面の簡単な説明

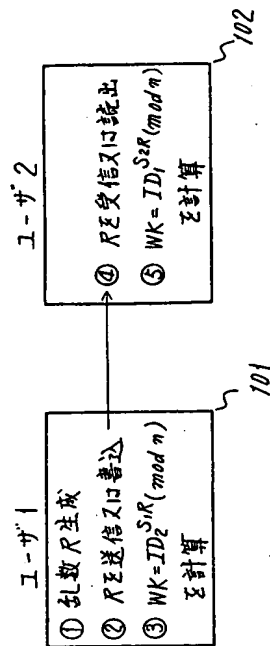
第1図は第1および第2の発明の実施例の原理を示すための図、第2図は第1の実施例の構成図、第3図は端末あるいはパソコンがなすべき作業のフローチャート、第4図は第2の実施例の構成図である。

101、102…ユーザ1、2がキー生成のた

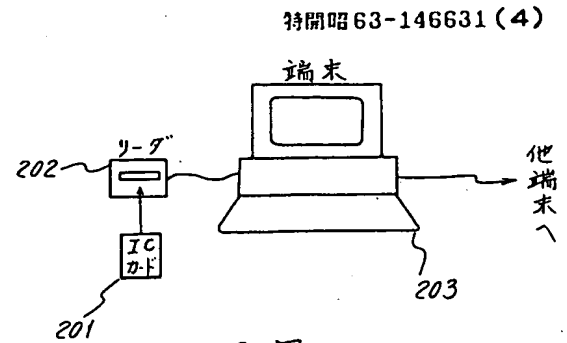
めに行なう処理、201、401…ICカード、202、402…リーダー、203…端末、403…パソコン。

代理人 弁理士 内 原



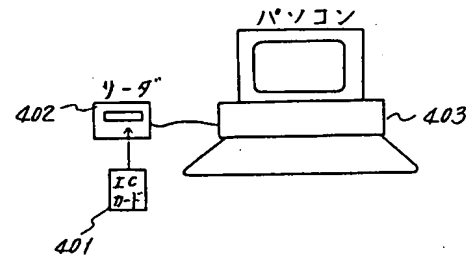


第1図



第2図

第4図



第3図

